REMARKS

Claims 1-9 and 11 are pending.

Claims 1, 3, 5-9 and 11 are rejected under 35 U.S.C. 102(e) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Malcolm et at., Pub. No.: US 2004/0078334 A1.

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Malcolm et al., Pub. No.: US 2004/0078334 A1 in view of Iitsuka et al. US Patent No. 6,463,151.

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Malcolm et al. Pub. No.: US 2004/0078334 A1 in view of Albrecht et al US Patent No. 6,510,521.

Reconsideration of the claims is requested.

In the Office Action, the Examiner cites a new reference, i.e., Malcolm et al. (US 2004/0078334A1), and asserts that Malcolm discloses the claimed invention.

The language of claim 1 requires ***whether or not the information is encrypted*** in accordance with the encryption rule by the information management system based upon the process information received over the network from the information management system. It appears in the Office Action the phrase "***whether or not the information is encrypted***" might be misinterpreted as whether the information needs to be encrypted. However, claim 1 intends that a monitoring portion monitors whether the information that has (already) been encrypted was encrypted according to the encryption rule. Claim 1 is amended for clarity by requiring "a monitoring portion that ***monitors by confirming whether*** ~~***or not***~~ ***the information management system encrypted the information*** ~~***is encrypted***~~ ***in accordance with the encryption rule*** ~~***by the information management system***~~ ***based upon the process information received over the network from the information management system.***"

The language of claim 1 requires an "***encryption support system***" and an "***information management system***."

The "***encryption support system***" requires the following:

A: **an encryption rule storing portion** that stores rule information that indicates an encryption rule for each secret level;

B: **an encryption data transmitting portion** that transmits encryption data that is necessary for encrypting the information in accordance with the encryption rule over the network to the information management system;

C: **a process information receiving portion** that receives process information, which indicates an encryption process performed by the information management system, over the network from the information management system;

D: **a monitoring portion** that ***monitors by confirming whether ~~or not~~ the information management system encrypted the information ~~is encrypted~~ in accordance with the encryption rule ~~by the information management system~~ based upon the process information received over the network from the information management system***; and

E: **a warning portion** that warns the information management system over the network, if the monitoring portion has determined that the information is not encrypted in accordance with the encryption rule.

The "***information management system***" requires the following:

F: **an encryption data receiving portion** that receives the encryption data over the network from the encryption support system;

G: **a classification secret level storing portion** that stores classification of the information in connection with a secret level for each classification;

H: **an encrypting portion** that specifies the classification of the information and encrypts the information by using the received encryption data of the secret level for the specified classification;

I: **an information storing portion** that stores the encrypted information; and

J: **a process information transmitting portion** that transmits the process information over the network to the encryption support system.

In particular, a feature of claim 1 is the combination of Element A (***an encryption rule storing portion***) and Element D (***a monitoring portion***). A feature of claim 1 is to define an encryption rule for each secret level and to monitor whether information has been encrypted based on the encryption rule.

The Examiner alleges that Malcolm discloses every single element of claim 1 of the present application. However, the language of claim 1 includes elements which Malcolm does not disclose, either expressly or implicitly. In particular, Malcolm fails to disclose, either expressly or implicitly, the combination of Element A and Element D discussed above, which is the feature of claim 1. Namely, the Office Action page 4 asserts that Malcolm teaches, in paragraph 0278, etc., Element D "a monitoring portion that ***monitors by confirming whether ~~or not~~ the information management system encrypted the information ~~is encrypted~~ in accordance with the encryption rule ~~by the information management system~~ based upon the process information received over the network from the information management system***."

However, an object monitored by "a monitoring portion" recited in claim 1 of the present application is different from an object monitored (checked) that is discussed in Malcolm. The language of amended claim 1 requires "***monitors by confirming whether ~~or not~~ the information management system encrypted the information ~~is encrypted~~ in accordance with the encryption rule***." In other words, the language of claim 1 expressly requires what is monitored is whether the information has been encrypted according to an encryption rule. In contrast, in Malcolm, what is monitored is whether information (e-mail message) needs to be encrypted from now on, as described in paragraph 0278. Paragraph 0278 discusses:

> In the next step S356, the e-mail message is checked to see whether or not it is to be encrypted.

In short, the present invention and Malcolm differ from each other in "***monitors by confirming whether ~~or not~~ the information management system encrypted the information ~~is encrypted~~ in accordance with the encryption rule ~~by the information management system~~ based upon the process information received over the network from the information management system***" as provided by the language of amended claim 1, and whether information ***is to be or needs to be encrypted from now*** as described by Malcolm.

Thus, it is readily apparent that a prima facie case of anticipation or obviousness based upon Malcolm cannot be established, because Malcolm fails to disclose either expressly or implicitly to one of ordinary skill in the art to modify Malcolm's checking of whether an email message needs to be encrypted to provide the claimed "***monitors by confirming whether ~~or not~~ the information management system encrypted the information ~~is encrypted~~ in accordance with the encryption rule ~~by the information management system~~ based upon***

***the process information received over the network from the information management system*.**" And Iitsuka and Albrecht have not been relied upon to disclose the discussed limitations of claim 1.

Withdrawal of the rejection of claim 1 and allowance of claim 1 is requested.

Independent claims 6, 8, 9 and 11 require limitations similar to the discussed limitations of claim 1.

The remaining dependent claims inherit the patentable recitations of their respective base claims, and therefore, patentably distinguish over the cited art for the reasons discussed above in addition to the additional features recited therein.

Independent Claim 5

Claim 5 corresponds to "an information management system" recited in claim 1 and the point of the invention claimed in claim 5 is, in particular, Element J, i.e., transmission of process information performed to encrypt to an encryption support system. Claim 5 is amended to require "[[a]]an encryption process ~~information~~ confirmation portion that confirms whether the encryption of the information was performed in accordance with the encryption rule by transmitting, over the network to the encryption support system, ~~portion that transmits~~ process information~~, which indicates~~ indicating the encryption process performed by the encrypting portion and receives a confirmation result from the encryption support system~~, over the network to the encryption support system~~ ~~so as to receive a check of whether the encryption of the information was performed in accordance with the encryption rule~~."

The Office Action page 5 asserts that Malcolm teaches, in paragraphs 0248 and 0275, and Fig. 17, a structure as defined by Element J. However, it is readily apparent that the relied upon Malcolm paragraphs and FIG. 17 are silent with regard to the structure as defined by amended Element J.

Withdrawal of the rejection of claim 5 and allowance of claim 5 is requested.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,
STAAS & HALSEY LLP

/Mehdi D. Sheikerz/

Date: _______July 17, 2009__________ By: ______________________________
Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Avenue, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501